RFC 2350 GRIM-CSIRT

EXPECTATION FOR COMPUTER SECURITY INCIDENT RESPONSE

TITLE: RFC 2350 GRIM-CSIRT
DATE: 10/07/2019
VERSION: 1.1
1 - DOCUMENT INFORMATION

1.1 Version
Version is 1.1

1.2 Distribution List
Notification of updates are submitted to the mailing list: soc[at]enav.it, cert[at]garr.it, soc[at]gse.it, cert[at]ncsc.fi.

1.3 Location where this document may be found
A copy of this document could be requested sending an email to csirt[at]grimaldi.napoli.it.
The current version of this document can be found at https://www.grimaldi.napoli.it/pdf/rfc-2350-grim-csirt.pdf

1.4 Authenticating this Document
This document has been signed with PGP key of GRIM-CSIRT. See section 2.8 for more details.

1.5 Document Identification
Title: "RFC 2350 GRIM-CSIRT"
Version: 1.1
Document Date: July 2019
Expiration: This document is valid until superseded by a later version
2 - CONTACT INFORMATION

2.1 Name of the team
Grimaldi Computer Security Incident Response Team
Short name: GRIM-CSIRT

2.2 Address
Postal Address
GRIM-CSIRT at Grimaldi EUROMED
Grimaldi EUROMED
Via Marchese Campodisola, 13
80133 - Napoli
Italy

2.3 Timezone
Central Europe Time/Central Europe Summer Time

2.4 Telephone number
+39 081 496787

2.5 Fax number
Fax number is provided for a restricted group of contacts.

2.6 Electronic email address
GRIM-CSIRT can be reached via csirt[at]grimaldi.napoli.it
All messages sent to this email address are received by all GRIM-CSIRT members.

2.7 Other telecommunications
None.
2.8 Public Keys and encryption information

PGP key is used for functional exchanges between GRIM-CSIRT and other parties:

ID: 0x638043EC

Fingerprint: 0411 FB29 16EE B23F 7A07 9700 054F 17F5 6380 43EC

2.9 Team members

GRIM-CSIRT is an Incident Response Team for the private sector Transportation & Logistic. It is operated by Grimaldi EUROMED a Grimaldi Group company. The team is made up of Cyber Security Analysts, Security Engineers and Incident Responders.

2.10 Other information

None.

2.11 Point of Customer Contact

The preferred method for contacting GRIM-CSIRT is via email at csirt[at]grimaldi.napoli.it. The mailbox is monitored during regular office hours: Monday to Friday, 08:30-17:30, except during public holiday in Italy. If you required urgent assistance, put "urgent" in your subject line or contact by telephone during regular office hours. Please, use PGP/GPG if you would be send sensitive information.
3 - CHARTER

3.1 Mission statement
GRIM-CSIRT's mission is to defend its constituency against cyber threat. Furthermore it suggests and implements security tactical and technical countermeasures in order to prevent and protect any violation attempt having an impact for Grimaldi information asset.

GRIM-CSIRT main targets are:
- Effective responsiveness in case of incidents and maximum commitment to resolve the issues.
- Provide information on potential threat impacting the information assets of Grimaldi Group.
- Facilitating the exchange of good practices between constituents and with peers.
- Increase the awareness and security culture for Grimaldi Group.

3.2 Constituency
GRIM-CSIRT constituency refers to the users, systems and applications and any other relevant resources of Grimaldi Group and all the companies belonging to the Group. Only vessels owned by "Grimaldi Euromed" and "Grimaldi Deep Sea" are included into constituency.

3.3 Sponsorship and/or affiliation
GRIM-CSIRT is managed by Security Team under control of Grimaldi EUROMED IT Department.

3.4 Authority
GRIM-CSIRT achieve its functions through the service delivered to its constituency, the collaboration with authoritative CERTs, peers, Information Security community, Law Enforcement and Service Providers.

GRIM-CSIRT is authoritative for "Grimaldi EUROMED" and "Grimaldi Deep Sea", meanwhile it acts as an advisory for all the other companies owned by Grimaldi Group: "Atlantic Container Line", "Malta Motorways of the Sea", "Minoan Lines" and "Finnlines".
4 - POLICIES

4.1 Types of Incidents and Level of Support
GRIM-CSIRT is authorized to address all types of information security incidents that occur within its constituency, according to agreements and mandates defined with constituency members. GRIM-CSIRT is also committed to keeping its constituency informed of relevant vulnerabilities, emerging threats and trends, and where possible, it will informs its community of such criticalities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information
GRIM-CSIRT receives incident reports related to events or threats impacting Grimaldi Group, then it classify and evaluates incident severity, and in accordance to triage, notify it to the appropriate management level. It also coordinates the activities needed to put in place appropriate incident resolutions. GRIM-CSIRT takes into account with regards to the handling and disclosure of information applicable laws of Italy, in order to not cause any injury.

GRIM-CSIRT shall exchanges all necessary information with other CSIRTs as well as with affected parties’ administrators. Neither personal nor further data are exchanged unless explicitly authorized.

4.3 Communication and Authentication
GRIM-CSIRT protects sensitive information in accordance with relevant regulations and policy within the EU.

Conventional method such as unencrypted emails are suitable for exchange of low sensitive information. To exchange high-sensitivity information an encrypted email with PGP/GPG keys is mandatory required.

GRIM-CSIRT recognize and support the ISTLP (Information Sharing Traffic Light Protocol). It will treat all submitted information as TLP:AMBER per default, and will only forward it to concerned constituency members or parties in order to resolve specific incidents when an acknowledge is implicit or expressly given.
5 - SERVICES

5.1 Incident Response
GRIM-CSIRT provide assistance and support to manage cyber security incidents impacting its constituency, offering reactive services such as incident triage, incident coordination artifact analysis and incident resolution.

5.1.1 Incident Triage
GRIM-CSIRT handles triage verifying the reliability of the source and finding any other available information. GRIM-CSIRT determining if an incident is authentic, assessing and prioritizing the incident.

5.1.2 Incident Coordination
GRIM-CSIRT coordinates incident management acting as described following:

1) Identifying constituency parties involved (owned company, internal department or team).
2) Establishing contacts with all the stakeholders in order to analyze the incident and identify actions to be undertaken.
3) Facilitating contacts with other involved parties that can provide support for solving the incident.
4) Promptly informing Grimaldi Management at the level corresponding to incident severity;
5) Writing reports and share it to other CERTs or interested organizations.

5.1.3 Incident Resolution
GRIM-CSIRT defines containment strategies, suggests and coordinates actions to contrast incident in order to ensure normal operations conditions as quickly as possible.

5.2 Proactive Services
GRIM-CSIRT provides information needed to protect Grimaldi Group's information assets.

GRIM-CSIRT aims to:

- Disseminate useful information for the growth of cyber security awareness of its constituency.
- Publish announcements concerning security threats relevant for its constituency.
- Provide and promote information exchange within peers and its constituency;
6 - INCIDENT REPORTING FORMS

All constituency members could report an incident via email to GRIM-CSIRT email address. In this case, it is necessary to provide as much more information as possible, such as:

- Date/time of event;
- Brief event description
- Involved actor or system (even potentially involved)
- Other.

Do not send malicious code or other attachments via email without having previously agreed with a GRIM-CSIRT team members.

7 - DISCLAIMER

GRIM-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.